JOURNAL OF COMBINATORIAL THEORY, Series A 63, 1–10 (1993)

Proof of a Conjecture on Hadamard 2-Groups

ROBERT G. KRAEMER

Department of Defense, Fort George G. Meade, Maryland 20755-6000

Communicated by the Managing Editors

Received February 1, 1989

By expanding on the results of James Davis, we prove by construction that every abelian 2-group that meets the exponent bound has a difference set.

1. INTRODUCTION

Let G be an arbitrary finite group of order v. A subset $D \subset G$ of size k is called a (v, k, λ)-*difference set* if every nonidentity element in G can be expressed in exactly λ ways as a "difference," $d_1 d_2^{-1}$, $d_1, d_2 \in D$.

Let G be an abelian 2-group. It is known from earlier work [6] that if G is to admit a nontrivial difference set, then the parameters (v, k, λ) can be assumed to be $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$ for some d. We also know [7] that the exponent of G, i.e., the smallest positive number m such that $g^m = 1$ for all $g \in G$, cannot be greater than 2^{d+2}. It is the purpose of this paper to show that the exponent bound is not only necessary, but also sufficient for G to admit a nontrivial difference set.

We begin with a review of some properties of characters on abelian 2-groups. A mapping, χ, from G into the complex numbers is called a *character* on G if $\chi(gh) = \chi(g)\chi(h)$ for all $g, h \in G$. It is clear that χ must take every element of G into a 2^mth root of unity, where 2^m is the exponent of G. For any abelian group there is always the trivial character which sends every element to 1. Such a mapping is called a *principal character*. In [5] the following basic result is shown:

LEMMA 1. *For any abelian group G, the characters of G form a group isomorphic to G.*

Now suppose that $D \subset G$ and $|D| = 2^{2d+1} - 2^d$. Then we have

LEMMA 2. *D is a difference set with parameters $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$, if and only if for every nonprincipal character χ, $|\sum_{d \in D} \chi(d)| = 2^d$.*

0097-3165/93 $5.00

Let H be any subgroup of G of order 2^{d+1}. We define an equivalence relation on the character group of G as

$$\chi \equiv \chi' \text{ if and only if } \operatorname{kern}(\chi) \cap H = \operatorname{kern}(\chi') \cap H.$$

The equivalence class associated to χ is denoted $[\chi]$. In particular, the equivalence class associated to the principal character χ_0 is denoted $[\chi_0]$. The following lemma due to Davis characterizes the equivalence class $[\chi]$.

LEMMA 3 (Davis). $[\chi] = \{\chi^a\gamma \mid$ *a is odd and* γ *is principal on* $H\}$. *Furthermore, if* χ' *is principal on* $\operatorname{kern}(\chi) \cap H$ *but not in* $[\chi]$, *then* $\chi' = \chi^{2a}\gamma$ *for some a and some* γ *principal on H.*

Proof. Suppose $\chi' = \chi^a\gamma$, where a is odd and γ is principal on H. Let $h \in H$ be such that $\chi(h) = 1$. Then clearly $\chi'(h) = 1$. Suppose that $\chi'(h) = 1$, then $\chi^a(h) = (\chi(h))^a = 1$. But since G is an abelian 2-group, there exists a unique minimal k so that $\chi(h)^{2^k} = 1$. Hence $2^k \mid a$. But a is odd; therefore k must be 0, and so $\chi(h) = 1$. Therefore $\chi \equiv \chi'$.

Now suppose that $\chi' \equiv \chi$. Let K be the $\operatorname{kern}(\chi) \cap H$. It is a trivial consequence of the isomorphism theorems for groups that $H \backslash K$ is cyclic, say, generated by hK. Since $\chi' \equiv \chi$, χ' is uniquely determined on H by where it sends h. Let the order of χ on H (and hence χ' on H) be 2^k. Then $\chi(h)$ is a primitive 2^kth root of unity, say ω. $\chi'(h)$ must also be a primitive 2^kth root of unity, else $\chi' \not\equiv \chi$. Hence $\chi'(h) = \omega^a$ for some odd a, which implies that on H, $\chi' = \chi^a$. Hence there exists a γ principal on H so that $\chi' = \chi^a\gamma$ on G.

Now suppose that χ' is a character which is principal on K, but not in $[\chi]$. As before, χ' is uniquely determined by where it sends h. Hence if $\chi(h) = \omega$ is a primitive 2^kth root of unity, then since χ' is principal on K, $\chi'(h)$ is a 2^jth root of unity for some $j \leqslant k$. But if $j = k$ then by the above $\chi' \in [\chi]$. Hence $j < k$, which implies that there is some even number $2a$ so that $\chi'(h) = \omega^{2a}$. Therefore on H we have $\chi' = \chi^{2a}$, which implies that there is a γ principal on H so that $\chi' = \chi^{2a}\gamma$ on G.

2. THE K-MATRIX

In the following sections we demonstrate how to construct a difference set in any abelian 2-group that meets the exponent bound. To do this we use a property of the group called a K-matrix structure, which was developed by James Davis and shown to exist in any abelian 2-group meeting the exponent bound of rank 2.

Let $[\chi_0], [\chi_1], \ldots, [\chi_Q]$ be a list of the distinct equivalence classes of the group characters of G. For each $[\chi_t]$, $t \neq 0$, let $K_t = \operatorname{kern}(\chi_t) \cap H$. Let h_t be

an element of $H\backslash K_t$ and let y_t and z_t be elements of $G\backslash H$. We associate to $[\chi_t]$ the $2^s \times 2^s$ matrix $M_t = (m_{i,j})$, where 2^{s+1} is the order of χ_t restricted to H, whose entries are in G and given by

$$m_{i,j} = y_t z_t^j h_t^{i-(2i+1)j}, \qquad 0 \leqslant i, j \leqslant 2^s - 1.$$

DEFINITION. The group G is said to possess a *K-matrix structure* if and only if the following three properties hold:

1. If χ is principal on K_t but $\chi \notin [\chi_t]$ or $[\chi_0]$, then the sum of the values of χ on any column of M_t is 0.

2. If $\chi \in [\chi_t]$, then the sum of the values of χ on any row of M_t is 0, except for one row, called i_0, which depends on χ, where the sum has magnitude 2^s = one-half the order of χ_t restricted to H.

3. The set $\{y_t z_t^j\}$, $0 \leqslant j \leqslant \frac{1}{2}|\chi_t|_H| - 1$, $1 \leqslant t \leqslant Q$, together with the identity, constitutes a complete set of distinct coset representatives of H in G.

In Davis' thesis [1] the following theorem is proved:

THEOREM 1 (Davis). *Any abelian 2-group that possesses a K-matrix structure has a difference set.*

In fact the difference set is easily constructed. For each $[\chi_t]$, $t \neq 0$, let D_t be the union of the cosets $m_{i,j}K_t$, where the $m_{i,j}$ are the entries in the associated K-matrix M_t. Let $\mathbf{D}$ be the union of all the D_t. Then $\mathbf{D}$ is the desired difference set in G. The proof involves checking that the character sums over $\mathbf{D}$ always have constant magnitude, namely 2^d, for each nonprincipal character χ.

Since the existence of a difference set is intimately related to the existence of appropriate h_t, y_t, and z_t's for each $t \geqslant 1$, it makes sense to investigate these elements more closely.

For what follows, assume that $[\chi_t]$ is given and that the order of $\chi_t|_H$ is 2^{s+1}, $s \geqslant 0$, and that $K_t = \ker(\chi_t) \cap H$.

LEMMA 4. *If $\chi \in [\chi_t]$, then for any $h \in H$, if $\chi_t(h)$ is a primitive 2^rth root of unity, so is $\chi(h)$.*

Proof. Without loss of generality we may assume that $\chi_t(h) = \omega$ and that $\chi(h) = \omega^{2^k a}$, where a is odd and ω is a primitive 2^rth root of unity. Then $\chi(h^{2^{r-k}}) = \omega^{2^r a} = 1$, which implies that $\chi_t(h^{2^{r-k}}) = 1$, which implies that ω is a 2^{r-k}th root of unity, which implies that $k = 0$.

LEMMA 5. *An h_t can always be found for all t, $1 \leqslant t \leqslant Q$, so that property 1 is satisfied.*

Proof. Recall that H/K_t is cyclic. Let h_tK_t generate H/K_t. Let χ be a character that is principal on K_t but not principal on H or in $[\chi_t]$. Then we know by Lemma 3 that $\chi = \chi_t^{2a}\gamma$, where γ is principal on H and χ_t^{2a} is not principal on H. For a fixed column j, the sum of the values of χ on the jth column of M_t is

$$\chi(y_t z_t^j h_t^{-j}) \sum_{i=0}^{2^s-1} \chi_t^{2a}(h_t^{1-2j})^i$$

which is zero, since $\chi_t(h^{2a(1-2j)})$ is a nontrivial 2^sth root of unity.

To find the y_t's and z_t's and to show that they are compatible with the h_t's chosen above, we need the following lemma.

LEMMA 6. *If $\chi \in [\chi_t]$ and $z \in G\backslash H$ such that $z^{2^m} \in H\backslash K_t$, then if $\chi_t(z)$ is a primitive 2^rth root of unity, so is $\chi(z)$.*

Proof. Without loss of generality, we may assume that $\chi_t(z) = \omega$, a primitive 2^rth root of unity and that $\chi(z) = \omega^{2^k a}$, a odd. Then $\chi(z^{2^m})$ is a 2^{r-k-m}th root of unity with $r > k+m$ (else z^{2^m} is in K_t). But by Lemma 4, this implies that $\chi_t(z^{2^m})$ is also a 2^{r-k-m}th root of unity (not necessarily primitive). Hence ω^{2^m} is a 2^{r-k-m}th root of unity, which implies that $k = 0$.

LEMMA 7. *For any group G meeting the exponent bound there exists a subgroup H of order 2^{d+1} so that we can always find z_t and an h_t for all t, $1 \leqslant t \leqslant Q$, that satisfy properties* 1 *and* 2 .

Proof. We break up the proof into two cases. First assume that $G = \mathbf{Z}_{2^{d+2}} \times A$, where A is any abelian 2-group of order 2^d. Let c be any element in $G\backslash A$ of order 2^{d+2} and set $H = A \times \langle c^{2^{d+1}} \rangle$. Let h_t be chosen as in Lemma 5; hence property 1 is satisfied. It remains to choose a z_t which is compatible with this h_t.

Let the order of χ_t restricted to H be 2^{s+1}. Note that s is always strictly less than d. Suppose that $c^{2^{d+1}} \notin K_t$. Then let $z_t = c^{2^{d-s+1}}$. Otherwise let $z_t = h_t c^{2^{d-s+1}}$. Clearly this z_t satisfies all the conditions of Lemma 6 with $m = s$. Hence for all $\chi \in [\chi_t]$ we have that $\chi(z)$ is a primitive 2^{s+1}th root of unity.

Now assume that the exponent of G is strictly less than 2^{d+2} and let $G = \mathbf{Z}_{2^{a_1}} \times \cdots \times \mathbf{Z}_{2^{a_k}} = A \times \mathbf{Z}_{2^{a_k}}$, where $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k \leqslant d+1$. Let H be any subgroup contained in A of order 2^{d+1} and let c be any element in $G\backslash A$ of order 2^{a_k}. Let the order of χ_t restricted to H be 2^{s+1}. Note that s is strictly less than a_k. Let $z_t = h_t c^{2^{a_k - s}}$. It is clear that z_t satisfies all the conditions of Lemma 6 with $m = s$. Hence for all $\chi \in [\chi_t]$ we have that $\chi(z)$ is a primitive 2^{s+1}th root of unity.

To check property 2, we need to show that

$$\sum_{j=0}^{2^s-1} \chi(y_t z_t^j h_t^{i-(2i+1)j}) = \chi(y_t h_t^i) \sum_{j=0}^{2^s-1} \chi(z_t h_t^{-(2i+1)})^j$$

is zero for any $\chi \in [\chi_t]$ for all i except one, called i_0, which depends on χ, in which case the sum has magnitude 2^s. From above, we have chosen z_t so that $\chi(z_t)$ is a primitive 2^{s+1}th root of unity for any $\chi \in [\chi_t]$ for any G meeting the exponent bound. Now by Lemma 4 we know that $\chi(h_t)$ is also a 2^{s+1}th primitive root of unity, call it ω. Let $\chi(z_t) = \omega^a$, where a is odd. Then $\chi(z_t h_t^{-(2i+1)}) = \omega^{a-2i-1}$. As long as $a - 2i - 1 \not\equiv 0 \bmod 2^{s+1}$, the sum is zero. At $2i \equiv a - 1 \bmod 2^{s+1}$, which has a unique solution modulo 2^s, we obtain $\sum_{j=0}^{2^s-1} \chi(z_t h_t^{-(2i+1)})^j = 2^s$. Since $\chi(y_t h_t^{i_0})$ is a root of unity, the sum has magnitude 2^s. Thus property 2 can always be satisfied.

3. Choosing the y_t's

It remains to show that there is a method for choosing y_t for all t given our choice of z_t and h_t such that property 3 is satisfied. We consider the case $\exp(G) = 2^{d+2}$ first.

Let $G = A \times \mathbf{Z}_{2^{d+2}}$, where A is some abelian 2-group and let c be any element in $G \backslash A$ of order 2^{d+2}. Recall that H is $A \times \langle c^{2^{d+1}} \rangle$. The cosets of H in G are H, cH, c^2H, ..., $c^{2^{d+1}-1}H$. Now for each t, z_t^j has the form $c^{j2^{d-s+1}}$ or $h^j c^{j2^{d-s+1}}$. Hence the only thing of interest is the exponent of c after multiplication by y_t, which is of the form c^{b_t}.

We begin by enumerating the distinct equivalence classes not equal to $[\chi_0]$ as $[\chi_1]$, $[\chi_2]$, ..., $[\chi_Q]$, so that the order of χ_t restricted to H is always greater than or equal to the order of χ_{t+1} restricted to H. We have the following useful fact concerning these Q equivalence classes:

Lemma 8. $\sum_{t=1}^{Q} |\chi_t|_H| = 2(2^{d+1} - 1)$.

Proof. By Lemma 3 we know that each equivalence class $[\chi_t]$ has exactly $\frac{1}{2}|\chi|_H|$ distinct elements when considered as characters on H. The sum is therefore merely asking for twice the total number of distinct nonprincipal characters on H, which is $2(2^{d+1} - 1)$.

We now choose y_t according to the following procedure:

1. Let $\mathscr{L}$ be an order list of integers from 1 to $2^{d+1} - 1$ all initially unmarked.

2. Set $t = 1$.

3. Let b_t be the minimal unmarked integer in $\mathscr{L}$. Mark all integers of the form $b_t + k2^{d-s+1}$, $0 \leqslant k \leqslant 2^s - 1$, where the order of χ_t restricted to H is 2^{s+1}.

4. Set $y_t = c^{b_t}$.

5. Increment t. Doing 3, 4, and 5 constitutes one step (step t). Go to 3 and repeat until Q steps have been taken.

The y_t's chosen in this manner satisfy property 3, provided we show the following three things:

LEMMA 9. 1. *We are never required to mark or choose an element outside of* $\mathscr{L}$.

2. *We never mark any integer in* $\mathscr{L}$ *more than once.*

3. *We eventually mark every integer in* $\mathscr{L}$.

Proof. First note that at step t me are marking out a number of integers equal to one-half the order of χ_t restricted to H. Hence by Lemma 8 we will make exactly $2^{d+1} - 1$ marks upon completion of the algorithm. Therefore at most $2^{d+1} - 1$ distinct integers in $\mathscr{L}$ will be marked.

To prove the first claim, it suffices to show that for all t, $1 \leqslant t \leqslant Q$, $b_t < 2^{d-s+1}$, where the order of χ_t restricted to H is 2^{s+1}. Suppose at step t that all the integers from 1 to $2^{d-s+1} - 1$ have been marked on previous steps. Let r be any integer in $\mathscr{L}$ not congruent to 0 mod 2^{d-s+1}. Then $r = r' + m2^{d-s+1}$, where $1 \leqslant r' \leqslant 2^{d-s+1} - 1$ and $0 \leqslant m \leqslant 2^s - 1$. But we are assuming that r' has already been marked. Hence there exists a $u < t$ so that $r' = b_u + m'2^{d-s'+1}$, where $s' \geqslant s$ and $m' \leqslant 2^{s'-s} - 1$. Hence $r = b_u + (m' + m2^{s'-s})\, 2^{d-s'+1}$. But since $m' \leqslant 2^{s'-s} - 1$ and $m \leqslant 2^s - 1$, we obtain $m' + m2^{s'-s} \leqslant 2^s - 1$. Therefore, r has been marked at an earlier step.

Now suppose that $b_t > 2^{d-s+1}$; i.e., suppose that 2^{d-s+1} has been marked on a previous step. Then there exists a $u < t$ and an $s' \geqslant s$, so that $2^{d-s+1} = b_u + m2^{d-s'+1}$ for some m strictly less than $2^{s'-s}$. But then if $k \leqslant 2^s - 1$, we have $k2^{d-s+1} = b_u + (2^{s'-s}(k-1) + m)\, 2^{d-s'+1}$. And since $2^{s'-s}(k-1) + m \leqslant 2^{s'-1}$, we have that $k2^{d-s+1}$ has been marked previously as well, which leaves no unmarked integer at step t. Therefore the algorithm must have ended previously; otherwise we contradict the fact that we make exactly $2^{d+1} - 1$ marks. Hence $b_t = 2^{d-s+1}$ and all the multiples of 2^{d-s+1} are the only remaining unmarked integers in $\mathscr{L}$. But step t requires that we make 2^s distinct marks. Since we have already made at least $2^{d+1} - (2^s - 1)$ marks on previous steps, this contradicts the fact that exactly $2^{d+1} - 1$ marks are made. Thus the first assertion is true.

To show the second claim, suppose that there is an integer r in $\mathscr{L}$ which is marked at least twice. Then there exist two distinct numbers t_1 and t_2 such that $r = b_{t_1} + m2^{d-s+1} = b_{t_2} + m'2^{d-s'+1}$, where as usual 2^{s+1} denotes the order of χ_{t_1} restricted to H and $2^{s'+1}$ denotes the order of χ_{t_2} restricted to$H$. Assume that $t_1 < t_2$; hence $s \geqslant s'$. Then we have that $2^{d-s+1} | b_{t_2} - b_{t_1}$. Hence we can write $b_{t_2} = b_{t_1} + k2^{d-s+1}$, for some $k > 0$. But by claim 1, b_{t_2} is in $\mathscr{L}$ and so $k \leqslant 2^s - 1$ and, therefore, b_{t_2} has already been marked at step t_1, contradicting the fact that it must be unmarked before step t_2.

The third claim follows at once from the remark made at the beginning of the proof and the first two claims.

We have demonstrated that h_t, z_t and y_t can always be chosen so that properties 1, 2, and 3 are satisfied for any abelian 2-group whose exponent is 2^{d+2} and hence we have shown:

THEOREM 2. *If G is an abelian 2-group with $\exp(G) = 2^{d+2}$, then G has a difference set.*

Now let us assume that the exponent on G is 2^e and write $G = A \times \mathbf{Z}_{2^e}$. Recall that H is chosen to be any order 2^{d+1} subgroup contained in A. Let $a_1, a_2, \ldots, a_m = 1$ be a complete set of $m = 2^{d+1-e}$ distinct coset representatives of H in A. Let c be any element of $G \backslash A$ of order 2^e. Recall that $z_t = h_t c^{2^{e-s}}$, where the order of χ_t restricted to H is 2^{s+1}, and that $s < e$ for all t. We choose y_t to be of the form $a_i c^j$, $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant 2^e$, with the proviso that y_t is never chosen to be the identity. Hence the only concern for satisfying property 3 is that as we run over all $t \geqslant 1$ the elements $a_{i_t} c^{j_t}$, $a_{i_t} c^{j_t + 2^{e-s}}, \ldots, a_{i_t} c^{j_t + (2^s - 1)2^{e-s}}$, together with the identity, comprise a complete set of coset representatives of H in G.

We begin by enumerating the equivalence classes exactly as before. Having done that, we write the cosets of H in an array thus:

$$\begin{pmatrix} a_1 cH & a_1 c^2 H & \cdots & a_1 c^{2^e - 1} H & a_1 H \\ a_2 cH & a_2 c^2 H & \cdots & a_2 c^{2^e - 1} H & a_2 H \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_m cH & a_m c^2 H & \cdots & a_m c^{2^e - 1} H & a_m H \end{pmatrix}.$$

The row indices run from 1 to m and the column indices run from 1 to 2^e.

The algorithm for choosing y_t is as follows:

1. Let $\mathscr{M}$ be an $m \times 2^e$ matrix of integers, each row of which contains the integers from 1 to 2^e in order, all initially unmarked.

2. Set $t = 1$.

3. Let b_t be the unmarked entry in $\mathscr{M}$ of minimal value. In case of a tie, choose the entry in the row of minimal index. Mark out all entries

in that row of the form $b_t + k2^{e-s}$, for $0 \leqslant k \leqslant 2^s - 1$, where 2^{s+1} is the order of χ_t restricted to H. Call the row where b_t lies r_t.

4. Set $y_t = a_{r_t} c^{b_t}$, where $a_m = 1$.

5. Increment t. Doing 3, 4, and 5 constitutes step t. Go to 3 and repeat until Q steps have occurred.

To show that when the y_t's are chosen in this manner property 3 is satisfied, it suffices to show the following lemma is true:

LEMMA 10. 1. *We are never forced to mark something outside of the matrix* $\mathcal{M}$.

2. *We never mark anything more than once.*

3. *Every entry except* $m_{m,2^e}$, *corresponding to the coset* H, *is marked.*

Proof. First note that the proof of Lemma 8 applies here as well. Hence we will never make more than a total of $2^{d+1} - 1$ marks upon completion of the algorithm.

To prove the first assertion it suffices to show that b_t is always less than or equal to 2^{e-s}, where 2^{s+1} is the order of χ_t restricted to H. Since by the remark above we will never mark out more than a total of $2^{d+1} - 1$ entries, we are never in the situation of having to step the algorithm, by not having any unmarked integer left in the array. So suppose we are at step t and $b_t > 2^{e-s}$. Let r be any integer, $1 \leqslant r \leqslant 2^e$, in row i. Then there exists an r', $0 < r' \leqslant 2^{e-s}$, so that $r = r' + k2^{e-s}$. Now, by assumption, r' has been previously marked; hence it is of the form $r' = b_u + k'2^{e-s'}$, where $s' \geqslant s$ and $k' < 2^{s'-s}$. Hence $r = b_u + (k' + 2^{s'-s}k)\, 2^{e-s'}$. But, since $k' \leqslant 2^{s'-s} - 1$ and $k \leqslant 2^s - 1$, we have $(k' + 2^{s'-s}k) \leqslant 2^{s'} - 1$, which implies that r has been previously marked. This holds for any i, since b_t had to be greater than 2^{e-s}. Hence every entry in $\mathcal{M}$ has been marked, contradicting the fact that at most $2^{d+1} - 1$ distinct entries can be marked.

To prove the second assertion, asume that there is some row where some integer r has been marked at least twice. Then there exists a t and a $t' > t$ so that $r = b_t + k2^{e-s} = b_{t'} + k'2^{e-s'}$, where 2^{s+1} is the order of χ_t, restricted to H, and $2^{s'+1}$ is the order of $\chi_{t'}$, restricted to H. Since $t' > t$ then $s' \leqslant s$. Therefore $b_{t'} - b_t$ is divisible by 2^{e-s}, which implies that there is some positive number q so that $b_{t'} = b_t + q2^{e-s}$. But, since $b_{t'} \leqslant b_t + k2^{e-s}$, then $q \leqslant k \leqslant 2^s - 1$, which implies that $b_{t'}$ had previously been marked, which is a contradiction.

To show the third assertion, note that since we mark at most $2^{d+1} - 1$ distinct entries and, by the above, we mark nothing more than once, we must mark exactly $2^{d+1} - 1$ entries in $\mathcal{M}$. Hence there is one entry which is not marked. Now if the integer 2^e in the mth row is marked, then there

exists a t and s, so that $2^e = b_t + k2^{e-s}$. But that can only occur if $b_t = 2^{e-s}$ and $k = 2^s - 1$. But this implies that every integer less than or equal to 2^{e-s} in all the rows has been previously marked. This, by an argument similar to the one used to prove the first assertion, implies that all the entries in $\mathcal{M}$ are marked after step t, contradicting the fact that exactly $2^{d+1} - 1$ entries are marked. Hence the third assertion is true. ∎

Thus, for any abelian 2-group with exponent less than 2^{d+2} we can always find an h_t, z_t, and y_t so that properties 1, 2, and 3 are satisfied. Combined with the result on groups of exponent 2^{d+2}, we have

THEOREM 3. *Any abelian 2-group that meets the exponent bound has a difference set.*

4. AN EXAMPLE

We will use the methods outlined above to construct a difference set in the group $\mathbf{Z}_4 \times \mathbf{Z}_4 \times \mathbf{Z}_{64}$. Let a, b, and c be the generators of G with $a^4 = b^4 = c^{64} = 1$. Since G has order 1024, the difference set D can be assumed to have parameters (1024, 496, 240). Since the exponent of G is 64, which is 2^{d+2}, we choose H to be the subgroup $\langle a \rangle \times \langle b \rangle \times \langle c^{32} \rangle$. Thus the cosets of H are H, cH, c^2H, ..., $c^{31}H$.

TABLE I

t	Class	Order	$\mathrm{Kern}(\chi_t) \cap H$	h_t	z_t	y_t
1	[0, 1, 0]	4	$\langle a \rangle \times \langle c^{32} \rangle$	b	bc^{16}	c
2	[0, 1, 1]	4	$\langle a \rangle \times \langle b^2c^{32} \rangle$	b	c^{16}	c^2
3	[1, 0, 0]	4	$\langle b \rangle \times \langle c^{32} \rangle$	a	ac^{16}	c^3
4	[1, 0, 1]	4	$\langle b \rangle \times \langle a^2c^{32} \rangle$	a	c^{16}	c^4
5	[1, 1, 0]	4	$\langle ab^3 \rangle \times \langle c^{32} \rangle$	a	ac^{16}	c^5
6	[1, 1, 1]	4	$\langle ab^3 \rangle \times \langle b^2c^{32} \rangle$	a	c^{16}	c^6
7	[1, 2, 0]	4	$\langle a^2b \rangle \times \langle c^{32} \rangle$	a	ac^{16}	c^7
8	[1, 2, 1]	4	$\langle a^2b \rangle \times \langle b^2c^{32} \rangle$	a	c^{16}	c^8
9	[1, 3, 0]	4	$\langle ab \rangle \times \langle c^{32} \rangle$	a	ac^{16}	c^9
10	[1, 3, 1]	4	$\langle ab \rangle \times \langle b^2c^{32} \rangle$	a	c^{16}	c^{10}
11	[2, 1, 0]	4	$\langle ab^2 \rangle \times \langle c^{32} \rangle$	b	bc^{16}	c^{11}
12	[2, 1, 1]	4	$\langle ab^2 \rangle \times \langle b^2c^{32} \rangle$	b	c^{16}	c^{12}
13	[0, 0, 1]	2	$\langle a \rangle \times \langle b \rangle$	—	—	c^{13}
14	[0, 2, 0]	2	$\langle a \rangle \times \langle b^2 \rangle \times \langle c^{32} \rangle$	—	—	c^{14}
15	[0, 2, 1]	2	$\langle a \rangle \times \langle bc^{32} \rangle$	—	—	c^{15}
16	[2, 0, 0]	2	$\langle a^2 \rangle \times \langle b \rangle \times \langle c^{32} \rangle$	—	—	c^{16}
17	[2, 0, 1]	2	$\langle b \rangle \times \langle ac^{32} \rangle$	—	—	c^{29}
18	[2, 2, 0]	2	$\langle ab \rangle \times \langle b^2 \rangle \times \langle c^{32} \rangle$	—	—	c^{30}
19	[2, 2, 1]	2	$\langle b \rangle \times \langle ac^{32} \rangle$	—	—	c^{31}

A character on G is uniquely determined by where it sends a, b, and c. Let ω be a primitive 64th root of unity and define $\chi_{r,s,t}(a^i b^j c^k)$ to be $\omega^{16ri+16sj+tk}$ for $0 \leqslant r \leqslant 3$, $0 \leqslant s \leqslant 3$, $0 \leqslant t \leqslant 63$. Then these are the 1024 distinct group characters on G.

We now collect these characters into equivalence classes. For convenience, the equivalence class of $[\chi_{r,s,t}]$ is simply denoted $[r, s, t]$. Table I summarizes the 19 distinct classes not equivalent to $[0, 0, 0]$.

The difference set is then formed by taking for $1 \leqslant t \leqslant 12$ the elements in the kernel and multiplying them by the elements $y_t z_t^j h_t^{i-(2i+1)j}$, where i and j go from 0 to 1 and for $13 \leqslant t \leqslant 19$, taking the elements in the kernel and multiplying them by y_t.

REFERENCES

1. J. A. DAVIS, "Difference Sets in Abelian 2-Groups," Thesis, University of Virginia, August 1987.
2. J. F. DILLON, Elementary Hadamard difference sets, *in* "Proceedings, 6th SCCGTC Congressus Numerantium XIV, 1975.
3. J. F. DILLON, On Hadamard difference sets, *Ars Combin.* **1** (1976).
4. M. HALL, "Combinatorial Theory," Blaisdell, Waltham, 1986.
5. W. LEDERMANN, "Introduction to Group Characters," Cambridge University Press, Cambridge, UK, 1977.
6. H. B. MANN, "Addition Theorems," Interscience, New York, 1965.
7. R. J. TURYN, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.